ANEXO I
PREGÃO ELETRÔNICO Nº 12/2022
Processo Administrativo nº 124/2022

TERMO DE REFERÊNCIA
(1ª Revisão)

1. DO OBJETO

1.1. Aquisição de solução integrada de segurança da informação, formada por equipamentos do tipo Firewall de Próxima Geração (*Next Generation Firewall* – NGFW), com licenças de *softwares*, suporte técnico e garantia pelo período de 36 (trinta e seis) meses, incluindo treinamento para utilização da solução, conforme as condições estabelecidas neste instrumento:

Grupo	Item	Descrição	Quant.	Unidade de medida
01	01	Firewall de Próxima Geração (*Next Generation Firewall* – NGFW), conforme especificações técnicas descritas no item 4 deste Termo de Referência.	2	Unidade
	02	Garantia e suporte técnico do fabricante da solução de NGFW	36	meses
	03	Licenças de Sistema de Relatoria e Log com suporte e garantia do fabricante.	36	meses
	04	Instalação e configuração da solução de NGFW	1	Serviço
	05	Treinamento oficial do fabricante da Solução de NGFW	2	Participante

1.2. O objeto da licitação tem a natureza de fornecimento de bens e serviços comuns, integrantes de Solução de *Firewall* de Nova Geração (NGFW).

1.3. Os quantitativos e respectivos códigos dos itens são os discriminados na tabela acima.

1.4. A presente contratação adotará como regime de execução a Empreitada por Preço Global.

1.5. O prazo de vigência do contrato é de 36 (meses, anos), podendo ser prorrogado por interesse das partes até o limite de 60 (sessenta) meses, com base no artigo 57, II, da Lei 8.666, de 1993.

2. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

2.1. A presente contratação se justifica pela necessidade substituição de equipamento de *Firewall* de tecnologia defasada por solução de segurança da informação de próxima geração (*Next Generation Firewall*), visando aprimorar a segurança no tráfego de informações e garantir uma maior estabilidade nos sistemas e aplicações, de modo a se alcançar um maior controle e gerenciamento nos serviços disponibilizados ao público usuário do Conselho.

3. CLASSIFICAÇÃO DOS BENS

3.1. Os bens e serviços a serem adquiridos e contratados estão definidos de forma objetiva, podendo ser licitados na modalidade Pregão Eletrônico, tendo em vista que se enquadram no conceito de bens e serviços comuns, nos termos do parágrafo único, do art. 1°, da Lei 10.520, de 2002.

4. DESCRIÇÃO DA SOLUÇÃO

4.1. A solução como um todo compreende o fornecimento de materiais (elementos de *hardware* e *software*) e serviços para a implantação de uma solução de Firewall de Próxima Geração no CREMERS.

4.2. O escopo contempla o fornecimento de equipamentos e licenças de softwares, instalação e configuração da solução, treinamento para utilização da solução fornecida, suporte técnico e garantia do fabricante, pelo período de 36 (trinta e seis) meses, para atualização do sistema operacional, correção de bugs, e troca do equipamento ou peças em caso de problema.

4.3. CARACTERÍSTICAS TÉCNICAS MÍNIMAS DOS EQUIPAMENTOS:

4.3.1. A solução deve consistir de *appliance* de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, *spywares* e *malwares* desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN;

4.3.2. O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

4.3.3. O equipamento deve ser fornecido com kit que permita a sua montagem em rack 19”;

4.3.4. Deve possuir *throughput* de, no mínimo, 2 (dois) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;

4.3.5. Deve possuir *throughput* de, no mínimo, 850 (oitocentos e cinquenta) Mbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os *throughput* aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;

4.3.6. Deve suportar, no mínimo, 190.000 (cento e noventa mil) conexões simultâneas;

4.3.7. Deve suportar, no mínimo, 35.000 (trinta e cinco mil) novas conexões por segundo;

4.3.8. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1 Gbps do tipo RJ-45;

4.3.9. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento;

4.3.10. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;

4.3.11. Deve possuir, no mínimo, 128 (cento e vinte e oito) GB de armazenamento interno para o sistema operacional e registro de logs;

4.3.12. Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 à 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento;

4.3.13. Deve suportar, no mínimo, 800 (oitocentos) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;

4.3.14. Deve suportar, no mínimo, 200 (duzentos) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;

4.3.15. Deve possuir suporte a criação de rede virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 1.000 (um mil) VLANs;

4.3.16. Deve implementar o protocolo LLDP – Link Layer Discovery Protocol;

4.3.17. Deve possuir o recurso de agregação de links conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um link agrupado virtualmente (LAG – Link Aggregation Group);

4.3.18. Deve possuir o recurso de NAT – Network Address Translation nas modalidades de NAT estático 1 para 1, NAT dinâmico 1 para vários e NAT dinâmico vários para vários. Este recurso deve ser aplicado tanto para o endereço de origem quanto para endereço de destino. Deve possuir também NAT64 para tradução entre endereços IPv6 e IPv4 e NPTv6 (Network Prefix Translation) para tradução de um prefixo IPv6 para outro prefixo IPv6 prevenindo problemas de roteamento assimétrico;

4.3.19. Deve suportar a criação de rotas estáticas e os protocolos de roteamento estático e dinâmico RIPv2, OSPFv2 e OSPFv3 incluindo OSPF graceful restart e BGP;

4.3.20. Deve implementar o protocolo ECMP – Equal Cost Multiple Path para balanceamento de carga entre links baseados no hash do endereço IP de origem, no hash do endereço IP de origem e de destino, pela técnica conhecida como round-robin e com base no peso ou prioridade atribuídos a cada link. Deve suportar o balanceamento entre, no mínimo 4 (quatro) links;

4.3.21. Deve permitir o envio de logs para sistemas de monitoração externos utilizando o padrão syslog, bem como o envio de forma segura através do protocolo SSL/TLS;

4.3.22. Deve possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo;

4.3.23. Deve implementar controle por políticas/regras de firewall capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego;

4.3.24. A identificação do país deve ser através do código do país, por exemplo, BR, USA, UK, RUS, etc e também através de geolocalização possibilitando a criação de regiões geográficas;

4.3.25. Deve permitir configurar o agendamento das políticas/regras de firewall para habilitar ou desabilitar tais políticas/regras em horários pré-definidos;

4.3.26. Deve possuir a capacidade para realizar a decriptografia do tráfego SSL e SSH permitindo o controle e inspeção tanto do tráfego de entrada quanto de saída. A decriptografia deve ser realizada com base em políticas/regras de acordo com a origem e destino do tráfego;

4.3.27. Deve possuir recurso de QoS – Quality of Service com suporte a DSCP – Differentiated Services Code Point. Deve permitir também definir, baseado em políticas/regras, a prioridade e o limite máximo de largura de banda de um determinado tipo de tráfego. As definições de prioridade e limite de largura de banda devem ser baseadas no endereço IP de origem e destino, no usuário e na aplicação;

4.3.28. Deve possuir a capacidade de reconhecer, no mínimo, 3.000 (três mil) aplicações diferentes tais como redes sociais, compartilhamento de arquivos, e-mail, atualização de softwares, acesso remoto, VoIP, áudio e vídeo, peer-to-peer, sistemas de mensagem instantânea, etc, sendo esta uma lista não exaustiva;

4.3.29. O reconhecimento da aplicação se dará, independentemente de porta e protocolo, através de, no mínimo, os seguintes métodos: baseado na assinatura da aplicação conhecida pelo fabricante da

solução de firewall, através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo e identificação através de análise heurística a fim de detectar aplicações através de análise comportamental do tráfego analisado;

4.3.30. Deve permitir a criação de assinaturas personalizadas para o reconhecimento de aplicações proprietárias na própria interface gráfica do equipamento sem a necessidade de intervenção do fabricante;

4.3.31. Deve permitir a diferenciação e controle de partes da aplicação como, por exemplo, em uma aplicação de mensagem instantânea permitir a troca de mensagens de texto e bloquear a transferência de arquivos por dentro da aplicação;

4.3.32. Deve permitir bloquear sessões TCP que utilizarem variações do three-way handshake como four-way e o five-way split handshake, prevenindo assim possíveis tráfegos maliciosos;

4.3.33. Deve permitir bloquear conexões que contenham dados no payload dos pacotes TCP SYN e TCP SYN-ACK durante o three-way handshake;

4.3.34. A solução de firewall deve possuir funcionalidades de IPS, antivírus e anti-spyware que permita o bloqueio de vulnerabilidades e exploits conhecidos e proteção contra vírus e spywares baseado em assinaturas de ameaças conhecidas;

4.3.35. Deve ser possível a criação de assinaturas customizadas de ameaças;

4.3.36. Deve permitir realizar o bloqueio de vírus realizando a inspeção em, no mínimo, os protocolos HTTP, FTP, SMB, SMTP e POP3. Será permitido o uso de *appliance* externo para o bloqueio de vírus caso a solução de firewall ofertada não realize nativamente a inspeção em algum dos protocolos solicitados;

4.3.37. Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2;

4.3.38. Deve possuir proteção contra ataques de negação de serviço (DoS) capaz de impedir ataques de SYN Flood, ICMP Flood, UDP Flood, etc e deve também bloquear port scans, bloquear ataques de buffer overflow e identificar e bloquear comunicação com botnets;

4.3.39. Para cada ameaça detectada pela solução deve ser realizado o registro nos logs do sistema das informações de data e hora, tipo da ameaça, origem e destino da comunicação e a ação tomada (se permitiu ou bloqueou o tráfego);

4.3.40. A solução de firewall deve possuir funcionalidade para análise de malwares não conhecidos (Malware Zero Day) onde o dispositivo envia o arquivo de forma automática para análise na “cloud” ou em um appliance instalado na rede local onde o arquivo será executado e simulado em um ambiente controlado (sandbox);

4.3.41. A solução de firewall deve possuir funcionalidade para análise de ameaças de comando e controle desconhecidas, sendo capaz de monitorar e bloquear a comunicação em tempo real através de HTTP, SSL, aplicações desconhecidas de tráfego TCP e UDP;

4.3.42. Deve possuir base de conhecimento em nuvem que permita compartilhar inteligência de ameaças em constante expansão. Deve ainda fornecer recursos de proteção avançados para tráfego DNS utilizando aprendizado de máquina através de análise comportamental com proteção baseada em nuvem para ação instantânea de bloqueio;

4.3.43. Caso seja fornecido um appliance local para análise de malwares não conhecidos ele deve

possuir, no mínimo, 28 (vinte e oito) ambientes controlados (sandbox) independentes para execução simultânea de arquivos suspeitos;

4.3.44. Caso seja necessário licença de sistema operacional e software para execução de arquivos no ambiente controlado (sandbox) as mesmas devem ser fornecidas em sua totalidade para o seu perfeito funcionamento;

4.3.45. O resultado da análise de malwares não conhecidos deve ter a capacidade de categorizar o arquivo analisado como, no mínimo, um arquivo malicioso, um arquivo não malicioso e um arquivo não malicioso, mas com características indesejáveis que deixam o sistema operacional lento ou que alteram parâmetros do sistema;

4.3.46. A análise de malwares não conhecidos deve ser realizada em arquivos trafegados na internet através dos protocolos HTTP, HTTPS e FTP bem como em arquivos trafegados entre servidores de arquivos utilizando o protocolo SMB. A análise também deve ser realizada em arquivos anexos em e-mails e links HTTP e HTTPS presentes no corpo de e-mails trafegados utilizando os protocolos SMTP e POP3. A análise do link HTTP e HTTPS presente no corpo do e-mail deve identificar se o website é um hospedeiro de exploits ou atividade de phishing;

4.3.47. Deve suportar a análise dos arquivos em ambientes controlados (sandbox) com, no mínimo, os sistemas operacionais MS Windows XP, MS Windows 7, MS Windows 10, MacOS e Linux;

4.3.48. A análise de malwares não conhecidos em ambiente controlado (sandbox) deve ser realizada em arquivos tipo executáveis, DLLs, arquivos compactados RAR e 7-ZIP, arquivos do pacote MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos PDF, arquivos JAVA (.jar e class), arquivos DMG e PKG, arquivos ELF e arquivos APK;

4.3.49. Deve atualizar a base de assinaturas para bloqueio dos malwares identificados no ambiente controlado (sandbox) dentro de, no máximo, 5 (cinco) minutos;

4.3.50. A solução de firewall deve possuir funcionalidade de filtro URL que permita a criação de políticas/regras para controle do acesso a websites baseado em categorias de URL devendo o fabricante da solução disponibilizar a base de dados de URL categorizadas para consulta por parte da solução. As políticas/regras que permitem ou bloqueiam o acesso a determinada categoria de URL devem ser com base no usuário e grupos de usuários e por endereços IP e faixas de endereços IP;

4.3.51. A funcionalidade de filtro URL deve possuir categoria específica para classificar domínios recém registrados com menos de 30 dias;

4.3.52. Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas;

4.3.53. Deve permitir a customização da página de bloqueio exibida ao usuário quando o mesmo tentar realizar um acesso a um website pertencente a uma categoria de URLs bloqueada;

4.3.54. Deve possuir recurso para proteger contra o roubo de credenciais de usuário e senha, identificadas através da integração com o Active Directory, submetidas em sites não corporativos. Deve ser possível definir em quais websites é permitido ou bloqueado o envio das credenciais baseado na categoria de URL a qual o website pertencer. Caso o usuário tente submeter suas credenciais de usuário e senhas pertencentes ao Active Directory em um website não autorizado deve ser exibido no web browser

do mesmo uma página de bloqueio informando que o uso de tais credenciais no website específico não está autorizado;

4.3.55. A solução de firewall deve possuir recurso que permita bloquear a transferência de arquivos baseado na extensão dos mesmos e também definir por qual aplicação a transferência do arquivo está bloqueada, por exemplo, bloquear a transferência de arquivos .exe através de web browser. Deve permitir bloquear, no mínimo, arquivo com as extensões .exe, .bat, .dll, .pif e .torrent;

4.3.56. A solução de firewall deve possuir integração com LDAP, MS Active Directoy e RADIUS para identificação dos usuários e grupos da rede para uso nas políticas/regras baseadas por usuários e grupo de usuários;

4.3.57. A integração com MS Active Directory para identificação dos usuários da rede deve ser realizada sem a necessidade de instalação de um agente no Controlador de Domínio e nem nas estações dos usuários;

4.3.58. A solução de firewall deve possuir recurso de portal de autenticação prévia (Captive Portal) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de software cliente ou agente no computador. O portal de autenticação deve ser exibido antes de o usuário iniciar a navegação pela internet;

4.3.59. A solução de firewall deve possuir o recurso de VPN – Virtual Private Network dos tipos site-to-site e client-to-site e suportar IPSEc – Internet Protocol Security e SSL – Secure Sockets Layer;

4.3.60. O recurso de VPN IPSec deve suportar os algoritmos de criptografia 3DES, AES 128, AES 192 e AES 256, os algoritmos de autenticação MD5 e SHA 1, o algoritmo IKEv1 e IKEv2 e os algoritmos de troca de chaves Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 e Grupo 14 e suportar também a autenticação através de certificados IKE PKI;

4.3.61. O recurso de VPN SSL deve permitir que o usuário remoto se conecte através de um software cliente de VPN instalado no sistema operacional do equipamento do usuário sendo possível a atribuição de endereços IP fixos e atribuição de DNS ao mesmo;

4.3.62. Deve suportar a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS Active Directory, TACACS+, RADIUS, SAML e através de base de usuários local no equipamento da solução de firewall. Deve suportar também a autenticação via certificado e OTP – One Time Password;

4.3.63. Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional MS Windows e MacOS;

4.3.64. A solução de firewall deve possuir console de gerenciamento do equipamento acessada através de interface gráfica web permitindo realizar as configurações da solução como criar e administrar as políticas/regras de firewall e controle de aplicações, criar e administrar as políticas de IPS, antivírus e anti-spyware, criar e administrar as políticas de filtro URL, monitorar e investigar os registros de logs de eventos e demais configurações;

4.3.65. Deve suportar a autenticação dos usuários administradores que se conectam à interface de gerenciamento do equipamento via LDAP, MS Active Directory, RADIUS e através de base de usuários local no equipamento da solução de firewall;

4.3.66. Deve ser possível criar perfis de acesso à interface de gerenciamento com permissões

granulares como acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações entre outros;

4.3.67. Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;

4.3.68. A interface de gerenciamento do equipamento deve possuir recurso para análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regas (shadowing) e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Deve possuir também recurso para análise das políticas indicando, quando houver, regras baseadas em porta e protocolo, permitindo a conversão da mesma para uma regra baseada em aplicação, melhorando assim o controle do tráfego e a segurança do ambiente. É permitido o uso de appliance externo para realização da análise das políticas, devendo o mesmo ser fornecido em conjunto com a solução de firewall e estar devidamente licenciado;

4.3.69. Deve ser possível através de interface de gerenciamento do equipamento a geração de relatórios tais como um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuário específicos incluindo aplicações e URLs acessadas e permitir a criação de relatórios personalizados;

4.3.70. Deve ser possível gerar relatório de visibilidade e uso das aplicações do tipo SaaS – Software as a Service mostrando os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso a aplicação SaaS e o consumo da aplicação SaaS pelo usuário;

4.3.71. Deve ser exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática a cada 1 (um) minuto, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU;

4.3.72. Deve ser possível configurar o envio de alertas do sistema via e-mail;

4.3.73. Deve suportar o monitoramento via SNMPv3;

4.3.74. O sistema operacional a ser instalado no equipamento que compõe a solução deverá ser fornecido em sua versão mais atualizada, não sendo aceito sistema operacional de uso genérico;

4.3.75. Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

4.3.76. Na data do certame, nenhum dos equipamentos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

4.3.77. Durante o período de vigência do contrato de garantia todos os componentes da solução de firewall, incluindo o equipamento, o sistema operacional do mesmo, as licenças necessárias para atender as funcionalidades e recursos solicitados, os softwares clientes de VPN e demais itens necessários para o perfeito funcionamento devem estar cobertos por garantia e suporte técnico do fabricante da solução em caso de problema;

4.3.78. A solução de firewall deve possuir garantia pelo período de, no mínimo, 36 (trinta e seis), compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e demais software e das assinaturas de proteção da solução.

4.4. SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO

4.4.1. A contratada deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos:

4.4.1.1. Reunião de alinhamento para criação do escopo do projeto previamente a instalação;

4.4.1.2. Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da contratante. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);

4.4.1.3. Análise da topologia e arquitetura da rede, considerando todos os equipamentos já existentes e instalados;

4.4.1.4. Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

4.4.1.5. Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;

4.4.1.6. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;

4.4.1.7. Configuração do sistema de firewall, VPN, IPS, Filtro URL, Antivírus e Anti-malware de acordo com as exigências levantadas;

4.4.2. Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos firewalls afim de garantir a melhor eficiência da solução durante o período de vigência das licenças;

4.4.3. Configuração do sistema de gerenciamento centralizado considerando adição dos novos appliances;

4.4.4. Repasse de informação das configurações realizadas no formato hands-on de 4 horas para a equipe responsável pelo projeto por parte da contratante após validação da migração;

4.5. TREINAMENTO OFICIAL DE FIREWALL DE PROXIMA GERAÇÃO

4.5.1. A contratada deverá disponibilizar, na quantidade indicada na descrição do objeto neste TR, *vouchers* individuais para participação de colaboradores indicados pelo CREMERS em treinamento oficial do fabricante do item de Solução de Segurança de Rede Firewall ofertado;

4.5.2. O treinamento deve ser ministrado abrangendo teoria e prática de configuração e administração de solução de firewall de próxima geração, bem como assuntos teóricos relacionados;

4.5.3. Deve conter, no mínimo, a seguinte ementa:

4.5.3.1. Arquitetura e Plataforma;

4.5.3.2. Configuração da Solução;

4.5.3.3. Políticas de Segurança e NAT;

4.5.3.4. Políticas de segurança baseada em aplicação;

4.5.3.5. Identificação de Aplicações;

4.5.3.6. Identificação de Usuário;

4.5.3.7. Bloqueio de ameaças;

4.5.3.8. Bloqueio de ameaças desconhecidas;

4.5.3.9. Bloqueio de ameaças em de tráfego criptografado;

4.5.3.10. Análise das informações de tráfego e ameaças detectadas;

4.5.3.11. Demais assuntos pertinentes a solução;

4.5.4. A duração do curso será de 5 dias em horário comercial;

4.5.5. Deve ser emitido um único certificado de conclusão cobrindo todo o curso para o participante;

4.5.6. O treinamento deverá ser ministrado pelo próprio fabricante ou por um parceiro nacional, capacitado, certificado e autorizado pelo fabricante a ministrar treinamentos oficiais;

4.5.7. O treinamento deve estar disponível na modalidade presencial nas instalações do fabricante ou da autorizada ou ministrado de forma remota;

4.5.8. O fabricante ou autorizada fornecerá os materiais didáticos para ministrar o curso;

4.5.9. Não será necessário considerar na proposta os custos de deslocamento, hospedagem e alimentação. Esses custos serão de responsabilidade da Contratante;

4.6. LICENÇAS DE SOFTWARES

4.6.1. Deverá ser fornecido certificado do fabricante que comprove o registro, no site do mesmo, do direito de atualização das licenças de softwares pelo período de 36 (trinta e seis);

4.6.2. O serviço de atualização das licenças de softwares será prestado dentro do período de garantia do contrato e consiste no fornecimento para o CREMERS de todas as versões*, features, releases, fixes* e *service packs*, de forma a manter a solução permanentemente atualizada, bem como, no fornecimento de manuais e boletins técnicos com informações que assegurem a plena utilização dos produtos licenciados e correções de erros *(bugs*) da solução sem ônus para o CREMERS.

4.7. GARANTIA E SUPORTE

4.7.1. Deve possuir garantia do fabricante com validade mínima de 36 (trinta e seis) meses;

4.7.2. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs;

4.7.3. Durante o prazo de garantia, deverá estar prevista a reposição de peças e equipamentos. Essa reposição deverá abranger todos os itens que compõem a solução, incluindo módulos ou outros equipamentos fornecidos pela Contratada para atendimento do edital;

4.7.4. Em caso de defeitos de fabricação ou a necessidade de substituição hardware, a garantia deve incluir envio de peças ou equipamentos de reposição nos locais especificados neste edital, obedecendo a modalidade NBD (Next Business Day);

4.7.5. Os chamados poderão ser abertos diretamente com o fabricante;

4.7.6. A empresa contratada deverá disponibilizar, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico ou website ou e-mail;

4.7.7. A contratada deverá disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana, com sistema de *help-desk* para abertura de chamados de suporte técnico;

4.7.8. A equipe técnica da contratante poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante login e senha de acesso ao sistema;

4.7.9. Todo chamado aberto deverá ter sua resolução técnica registrada no sistema *web* de *help-desk*;

4.7.10. A contratada deverá prestar o suporte técnico dos produtos, sendo facultado a ela o escalonamento das questões para o respectivo fabricante, ficando, entretanto, a contratada responsável pelo gerenciamento do chamado e prestação de informações à contratante;

4.7.11. A contratada deve indicar, por ocasião do início dos trabalhos, os procedimentos para abertura de suporte técnico;

4.7.12. As horas de atendimento serão realizadas normalmente em horário comercial, no período compreendido entre 08:00 e 18:00h, em dias de semana (segunda à sexta).

4.8. PADRONIZAÇÃO

4.8.1. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), os equipamentos e softwares deste lote/grupo, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante;

4.9. HABILITAÇÃO E QUALIFICAÇÃO DO FORNECEDOR

4.9.1. Deve ser apresentado atestado de capacidade técnica comprovando que a licitante é apta a instalar, configurar e prestar suporte técnico das soluções referente a este edital;

4.9.2. A contratada deverá possuir, pelo menos, um técnico certificado pelo fabricante compatível com o objeto deste termo de referência;

4.9.2.1. A comprovação de vínculo profissional se fará com a apresentação de cópia da carteira de trabalho (CTPS) em que conste o licitante como contratante; do contrato social do licitante em que conste o profissional como sócio; do contrato de prestação de serviços, sem vínculo trabalhista, regido pela legislação civil ou, ainda, de declaração de contratação futura do profissional, desde que acompanhada de declaração de anuência do profissional.

4.10. CONDIÇÕES GERAIS

4.10.1. Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital. Em caso de dúvida ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnico certificado na solução para configuração e comprovação dos itens pendentes, nas dependências deste órgão (conforme itens 1.1.1 e 1.1.2, TC-006.806/2006-4, Acórdão nº 838/2006-TCU-2ª Câmara);

5. ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO.

5.1. O prazo de entrega do objeto, incluindo a instalação e configuração da solução, é de até 120 (cento e vinte) dias corridos, a partir da data de assinatura do contrato.

5.1.1. Os equipamentos devem ser entregues no seguinte endereço: Av. Princesa Isabel, 921, bairro Santana – Porto Alegre / RS – CEP 90620-001, mediante agendamento com antecedência mínima de 24 horas, sob o risco de não ser autorizada;

5.2. Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local para download do arquivo de instalação;

5.3. Somente serão aceitos equipamentos novos e sem uso. Não serão aceitos equipamentos re-manufaturados, NFR (Not For Resale) ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

5.4. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 (quinze) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

5.5. O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente especificação técnica;

5.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

6. OBRIGAÇÕES DA CONTRATANTE

6.1. Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

6.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

6.3. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

6.4. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;

6.5. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;

6.6. A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do objeto, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

7. OBRIGAÇÕES DA CONTRATADA

7.1. A CONTRATADA deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

7.2. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo e prazo de garantia ou validade;

7.2.1. Os equipamentos devem estar acompanhados do manual do usuário, com uma versão em português e da relação da rede de assistência técnica autorizada;

7.3. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

7.4. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

7.5. Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

7.6. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

7.7. Indicar preposto para representá-la durante a execução do contrato.

7.8. Prestar garantia de todos os equipamentos adquiridos e instalação dos mesmos pelo prazo mínimo estabelecido neste Termo de Referência.

7.9. Arcar com todas as despesas com tributos, fretes, tarifas e as despesas decorrentes da execução do objeto, sem qualquer ônus ao CONTRATANTE.

8. DA SUBCONTRATAÇÃO

8.1. Não será admitida a subcontratação do objeto licitatório.

9. DA ALTERAÇÃO SUBJETIVA

9.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

10. DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

10.1. Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

10.1.1. O recebimento de material de valor superior a R$ 176.000,00 (cento e setenta e seis mil reais) será confiado a uma comissão de, no mínimo, 3 (três) membros, designados pela autoridade competente.

10.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

10.3. O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

11. DO PAGAMENTO

11.1. O pagamento será realizado no prazo máximo de até 15 (quinze) dias, contados a partir do recebimento da Nota Fiscal ou Fatura, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

11.1.1. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

11.2. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

11.3. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

11.3.1. Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

11.4. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a contratada providencie as medidas saneadoras. nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o contratante.

11.5. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

11.6. Antes de cada pagamento à CONTRATADA, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

11.7. Constatando-se a irregularidade da Contratada junto ao SICAF, será providenciada sua notificação, por escrito, para que, no prazo de 5 dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante.

11.8. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

11.9. Não havendo regularização ou sendo a defesa considerada improcedente, o CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

11.10. Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

11.11. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.

11.11.1. Será rescindido o contrato em execução com a CONTRATADA inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade do CONTRATANTE.

11.12. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

11.12.1. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

11.13. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) \qquad I = \frac{(6 / 100)}{365} \qquad I = 0{,}00016438$$

TX = Percentual da taxa anual = 6%

12. DO REAJUSTE

12.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

12.2. Após o interregno de um ano, e independentemente de pedido da CONTRATADA, os preços iniciais serão reajustados, mediante a aplicação, pela CONTRATANTE, do Índice Nacional de Preços ao Consumidor – INPC –, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, com base na seguinte fórmula (art. 5º do Decreto n.º 1.054, de 1994):

R = V (I – Iº) / Iº, onde:

R = Valor do reajuste procurado;

V = Valor contratual a ser reajustado;

Iº = índice inicial - refere-se ao índice de custos ou de preços correspondente à data fixada para entrega da proposta na licitação;

I = Índice relativo ao mês do reajustamento;

12.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

12.4. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajuste de preços do valor remanescente, sempre que este ocorrer.

12.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

12.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

12.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

12.8. O reajuste será realizado por apostilamento.

13. GARANTIA DA EXECUÇÃO

13.1. Não haverá exigência de garantia contratual da execução, pelas razões abaixo justificadas:

13.1.1. Não se trata de execução de serviço com dedicação de mão de obra exclusiva;

13.1.2. Pela forma de pagamento, que acontece somente após o ateste da Nota Fiscal pelo Gestor do CONTRATO, não há risco para Administração;

13.1.3. No Mapa de Risco não foi identificada ações preventivas ou de contingência que pudessem ser sanados com a utilização da garantia contratual.

14. GARANTIA CONTRATUAL DOS BENS

14.1. O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, 36 (trinta e seis), ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

14.2. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o CONTRATANTE.

14.3. A garantia abrange a realização da manutenção corretiva dos bens pela própria Contratada, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

14.4. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

14.5. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

14.6. Uma vez notificada, a Contratada realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 10 (dez) dias úteis, contados a partir da data de retirada do equipamento das dependências da Administração pela Contratada ou pela assistência técnica autorizada.

14.7. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da Contratada, aceita pelo Contratante.

14.8. Na hipótese do subitem acima, a CONTRATADA deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo CONTRATANTE, de modo a garantir a continuidade dos trabalhos durante a execução dos reparos.

14.9. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do CONTRATANTE ou a apresentação de justificativas pela CONTRATADA, fica o CONTRATANTE autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de

seus componentes, bem como a exigir da CONTRATADA o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

14.10. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da CONTRATADA.

14.11. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

15. DAS SANÇÕES ADMINISTRATIVAS

15.1. Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a CONTRATADA que:

15.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

15.1.2. ensejar o retardamento da execução do objeto;

15.1.3. falhar ou fraudar na execução do contrato;

15.1.4. comportar-se de modo inidôneo;

15.1.5. cometer fraude fiscal;

15.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

15.2.1. Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

15.2.2. multa moratória de 0,2 % (dois décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta dias) dias;

15.2.3. multa compensatória de 10 % (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

15.2.4. em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

15.2.5. suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

15.2.6. Sanção de impedimento de licitar e contratar com órgãos e entidades da União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

15.2.6.1. A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa neste Termo de Referência.

15.2.7. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir o CONTRATANTE pelos prejuízos causados;

15.3. As sanções previstas nos subitens 15.2.1, 15.2.5, 15.2.6 e 15.2.7 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

15.4. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

15.4.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

15.4.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

15.4.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

15.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

15.6. As multas devidas e/ou prejuízos causados ao CONTRATANTE serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

15.6.1. Caso o CONTRATANTE determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

15.7. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

15.8. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

15.9. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização.

15.10. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

15.11. O processamento do Processo Administrativo de Responsabilização – PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

15.12. As penalidades serão obrigatoriamente registradas no SICAF.

16. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

16.1. As exigências de habilitação jurídica e de regularidade fiscal e trabalhista são as usuais para a generalidade dos objetos, conforme disciplinado no Edital.

16.2. Os critérios de qualificação econômico-financeira a serem atendidos pelo fornecedor estão previstos no edital.

16.3. Os critérios de qualificação técnica a serem atendidos pelo fornecedor serão:

16.3.1. Comprovação de aptidão para o fornecimento de bens em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

16.3.1.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas: instalação, configuração e prestação de suporte técnico de soluções de NGFW – Firewall de Próxima Geração – de especificações mínimas compatíveis com as descritas neste Termo de Referência;

16.3.2. A contratada deverá comprovar que possui em seu quadro funcional, pelo menos, um técnico certificado pelo fabricante compatível com o objeto deste termo de referência;

16.3.2.1. A comprovação de vínculo profissional se fará com a apresentação de cópia da carteira de trabalho (CTPS) em que conste o licitante como contratante; do contrato social do licitante em que conste o profissional como sócio; do contrato de prestação de serviços, sem vínculo trabalhista, regido pela legislação civil ou, ainda, de declaração de contratação futura do profissional, desde que acompanhada de declaração de anuência do profissional.

16.4. Os critérios de aceitabilidade e julgamento da proposta é o Menor Preço Global dos itens, conforme tabela constante deste Termo de Referência.

17. ESTIMATIVA DE PREÇOS E PREÇOS REFERENCIAIS.

17.1. O valor de referência para a contratação será o seguinte:

Descrição/Especificação	**Valor unit.**	**Qtde**	**Valor total**
Firewall de Próxima Geração (NGFW) com suporte técnico especializado e garantia do fabricante, incluindo atualização do sistema operacional e licenças de *Softwares* de Relatoria e Log, pelo período de 36 (trinta e seis) meses,	R$ 52.877,79	2	R$ 105.755,58
Instalação e Configuração da Solução de NGFW	R$ 33.535,84	1	R$ 33.535,84
Participação em Treinamento Oficial do Fabricante da Solução de NGFW	R$ 22.225,26	2	R$ 44.450,52
Valor Total da solução de NGFW			**R$ 183.741,94**

18. DOS RECURSOS ORÇAMENTÁRIOS.

18.1. Os recursos para a contratação estão previstos em orçamento próprio do Conselho Regional de Medicina do Estado do Rio Grande do Sul, nas dotações orçamentárias 6.2.2.1.2.44.90.52.004 – Equipamentos de Informática, e 6.2.2.1.1.33.90.39.025 – Serviços de Seleção, Treinamento e Aperfeiçoamento.

19. DAS CONSIDERAÇÕES FINAIS

19.1. As normas que disciplinam este procedimento serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

19.2. Aos casos omissos aplicar-se-ão as demais disposições constantes da Lei nº 8.666/93, com suas posteriores alterações e legislação correlata.

Porto Alegre, 06 de setembro de 2022.

Esequiel Steil
Comissão Permanente de Licitação

Ricardo de Azevedo Pereira
Coordenador de TI